



Control theorems for fine Selmer groups, and duality of fine Selmer groups attached to modular forms

Jeffrey Hatley¹ · Debanjana Kundu² · Antonio Lei³  · Jishnu Ray⁴

Received: 11 November 2021 / Accepted: 25 January 2022

© The Author(s), under exclusive licence to Springer Science+Business Media, LLC, part of Springer Nature 2022

Abstract

Let \mathcal{O} be the ring of integers of a finite extension of \mathbb{Q}_p . We prove two control theorems for fine Selmer groups of general cofinitely generated modules over \mathcal{O} . We apply these control theorems to compare the fine Selmer group attached to a modular form f over the cyclotomic \mathbb{Z}_p -extension of \mathbb{Q} to its counterpart attached to the conjugate modular form \bar{f} .

Keywords Fine Selmer groups · Control theorems · Conjugate modular forms

Mathematics Subject Classification Primary 11R23 · Secondary 11F11, 11R18

1 Introduction

Let p be a fixed odd prime number. Let f be a normalized eigen-cuspform of level N and weight $k \geq 2$. We assume throughout that $p \nmid N$. We write \bar{f} for its conjugate modular form, that is, the modular form whose Fourier coefficients are given by the complex conjugation of those of f . We fix embeddings $\iota_\infty : \overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$ and $\iota_p : \overline{\mathbb{Q}} \hookrightarrow \mathbb{C}_p$, which allow us to regard the Fourier coefficients of f and \bar{f} as elements of \mathbb{C}_p . Let K/\mathbb{Q}_p be a fixed finite extension that contains all these Fourier coefficients and write \mathcal{O} for its ring of integers. Throughout, ϖ is a fixed uniformizer of \mathcal{O} .

DK acknowledges the support of the PIMS postdoctoral fellowship. AL is supported by the NSERC Discovery Grants Program RGPIN-2020-04259 and RGPAS-2020-00096. JR acknowledges postdoctoral research support from the Tata Institute of Fundamental Research, Mumbai during the later stage of preparing this article. Parts of this work were carried out during the thematic semester “Number Theory—Cohomology in Arithmetic” at Centre de Recherches Mathématiques (CRM) in fall 2020. DK, AL, and JR thank the CRM for the hospitality and generous supports.

✉ Antonio Lei
antonio.lei@mat.ulaval.ca

Extended author information available on the last page of the article

For $g = f$ or \bar{f} , let V_g denote the K -adic $G_{\mathbb{Q}}$ -representation attached to g by Deligne [5]. Our normalization is such that these representations have Hodge–Tate weights 0 and $1 - k$ at p , with the convention that the p -adic cyclotomic character has Hodge–Tate weight 1. Recall that the K -linear dual of V_f is

$$V_f^* := \text{Hom}_K(V_f, K) \cong V_{\bar{f}}(k - 1),$$

where $M(j)$ denotes the j -th Tate twist of a $G_{\mathbb{Q}}$ -module M for $j \in \mathbb{Z}$. Fix a Galois-stable \mathcal{O} -lattice T_f inside V_f and define an \mathcal{O} -lattice $T_{\bar{f}}$ inside $V_{\bar{f}}$ to be

$$T_{\bar{f}} := \text{Hom}_{\mathcal{O}}(T_f, \mathcal{O})(1 - k).$$

For $g = f$ or \bar{f} , we write $A_g = V_g/T_g$.

We write \mathbb{Q}_{cyc} for the cyclotomic \mathbb{Z}_p -extension of \mathbb{Q} and let Γ denote the Galois group $\text{Gal}(\mathbb{Q}_{\text{cyc}}/\mathbb{Q})$. Suppose L_n is the unique finite subextension of \mathbb{Q}_{cyc} with Galois group over \mathbb{Q} of order p^n . Suppose $L_{n,p}$ is the completion of L_n at the unique place above p . The Iwasawa algebra $\Lambda = \mathcal{O}[[\Gamma]]$ is defined to be $\varprojlim \mathcal{O}[\Gamma/\Gamma_n]$, where $\Gamma_n = \Gamma^{p^n}$ and the connecting maps are projections. After fixing a topological generator γ of Γ , there is an isomorphism of rings $\Lambda \cong \mathcal{O}[[X]]$, by sending γ to $X + 1$. Given a Λ -module M , denote its Pontryagin dual by $M^\vee := \text{Hom}_{\mathcal{O}}(M, K/\mathcal{O})$.

We recall the notion of *fine Selmer groups* (which is denoted by Sel_0 in the present article) defined by Coates and Sujatha in [3] (see also [22]). This is a subgroup of the classical Selmer group obtained by imposing stronger vanishing conditions at primes above p (the precise definition is reviewed in §2 below). A deep result of Kato shows that the fine Selmer group over \mathbb{Q}_{cyc} is always cotorsion as a Λ -module regardless of whether f is ordinary at p or not, a fact that is not true for classical Selmer groups. Based on results of Kato in [9] and Perrin-Riou [16], it has been shown in [11, Proposition 6.3] that classical Selmer groups are not Λ -cotorsion when p is a good nonordinary prime. See also [4, Theorem 2.6]. Fine Selmer groups can also be used to formulate an Iwasawa Main Conjecture for modular forms without p -adic L -functions [9, Conjecture 12.10]; this fact can also be exploited while working with Coleman families of modular forms where the signed Selmer groups are unavailable. A formulation of an Iwasawa Main Conjecture without p -adic L -functions for universal deformations is given in [15, Section 5].

In this article, we shall prove two control theorems for fine Selmer groups. The first one concerns passing between the fine Selmer group of the ϖ^e -torsion of a cofinitely generated \mathcal{O} -module and the ϖ^e -torsion of the fine Selmer group of the whole module.

Theorem A (Theorem 3.2) *Let $e \geq 1$ be fixed integers and M a cofinitely generated \mathcal{O} -module equipped with a continuous $G_S(\mathbb{Q})$ -action. Let \mathcal{F} be a subfield of \mathbb{Q}_{cyc} . Then the natural map*

$$r : \text{Sel}_0(M[\varpi^e]/\mathcal{F}) \longrightarrow \text{Sel}_0(M/\mathcal{F})[\varpi^e]$$

has finite kernel and cokernel with order bounded independently of e .

The second control theorem concerns passing between fine Selmer groups over \mathbb{Q}_{cyc} and L_n . It is divided into two parts. The first part studies the fine Selmer groups of ϖ^e -torsion of a general cofinitely generated \mathcal{O} -module. The second part studies the fine Selmer groups attached to modular forms. Let $F \in \Lambda$ be an irreducible polynomial. Let $g = f$ or \bar{f} , and $j \in \mathbb{Z}$. We write $A_g(j)_{F^m}$ for the tensor product $A_g(j) \otimes_{\mathcal{O}} \Lambda/F^m$, equipped with the diagonal Galois action.

Before discussing a crucial hypothesis, which we call $(H\text{-base}_F)$, we introduce some notation. Let ι denote the involution on Λ sending a group-like element of Γ to its inverse. For any Λ -module M , we write M^ι for the Λ -module which coincides with M as a \mathbb{Z}_p -module, with the action of Γ given by

$$\gamma \cdot_\iota x = \gamma^{-1}x \quad \text{for } \gamma \in \Gamma \text{ and } x \in M.$$

Hypothesis $(H\text{-base}_F)$: For all $v|N$, the cohomology group $H^0(\mathbb{Q}_v, A_g(j) \otimes_{\mathcal{O}} \Lambda/\mathcal{F})$ is finite for $(g, j, \mathcal{F}) = (f, i, F)$ and $(\bar{f}, k - i, F^\iota)$.

We can now state our second control theorem:

Theorem B (Theorem 3.7) *Let M be a cofinitely generated \mathcal{O} -module equipped with a continuous action of $G_S(\mathbb{Q})$. Let $n \geq 0$ be an integer.*

(i) *Let $e \geq 1$ be an integer. Then, the kernel and cokernel of the restriction map*

$$r_n : \text{Sel}_0(M[\varpi^e]/L_n) \longrightarrow \text{Sel}_0(M[\varpi^e]/\mathbb{Q}_{\text{cyc}})^{\Gamma_n}$$

are finite and bounded independently of n .

(ii) *Let F be a fixed irreducible distinguished polynomial and $m \geq 1$ an integer. Suppose that $M = A_f(i)_{F^m}$ or $A_{\bar{f}}(k - i)_{F^{\iota,m}}$ and that $(H\text{-base}_F)$ holds. Then, the kernel and cokernel of the restriction map*

$$r : \text{Sel}_0(M/\mathbb{Q}) \longrightarrow \text{Sel}_0(M/\mathbb{Q}_{\text{cyc}})^{\Gamma}$$

are finite.

Our results are slightly more general than those proven by Rubin in [17, Proposition 7.4.4] (see also [12, 21] for similar control theorems for fine Selmer groups of abelian varieties). We utilize our control theorems to study the Λ -structure of $\text{Sel}_0(A_g(j)/\mathbb{Q}_{\text{cyc}})^\vee$ under duality. More precisely, we study links between $U := \text{Sel}_0(A_f(i)/\mathbb{Q}_{\text{cyc}})^\vee$ and $V := \text{Sel}_0(A_{\bar{f}}(k - i)/\mathbb{Q}_{\text{cyc}})^\vee$. The twists we consider originate from the perfect pairing of $G_{\mathbb{Q}}$ -modules

$$T_f(i) \times T_{\bar{f}}(k - i) \longrightarrow \mathcal{O}(1).$$

For any finitely generated Λ -torsion module M , we denote its F^∞ -torsion (resp. ϖ^∞ -torsion) part appearing in the pseudo-isomorphism between M and cyclic Λ -modules by $M(F^\infty)$ (resp. $M(\varpi^\infty)$) (see §2). In this article, we provide necessary and sufficient conditions for the equalities $U(F^\infty) = V(F^\infty)$ and $U(\varpi^\infty) = V(\varpi^\infty)$ in terms of growth conditions of the following localization maps:

$$\begin{aligned} \theta_{F,m,e} &: H^1(G_S(\mathbb{Q}), A_f(i) \otimes_{\mathcal{O}} \Lambda/F^m[\varpi^e]) \longrightarrow H^1(\mathbb{Q}_p, A_f(i) \otimes_{\mathcal{O}} \Lambda/F^m[\varpi^e]), \\ \theta_{n,e} &: H^1(G_S(L_n), A_f(i)[\varpi^e]) \longrightarrow H^1(L_{n,p}, A_f(i)[\varpi^e]). \end{aligned}$$

Our control theorems allow us to prove the following:

Theorem C *Under the notation introduced above, we have*

- (i) *Let $F \in \Lambda$ be an irreducible distinguished polynomial such that $(H\text{-base}_F)$ holds. Then, $U(F^\infty) = V(F^\infty)$ if and only if*

$$|\text{Image}(\theta_{F,m,e})| \sim_e q^{e \deg(F^m)} \quad \text{for all integers } m \geq 1.$$

- (ii) *We have $U(\varpi^\infty) = V(\varpi^\infty)$ if and only if*

$$|\text{Image}(\theta_{n,e})| \sim_n q^{ep^n} \quad \text{for all integers } e \geq 1.$$

In particular, U and V have equal μ -invariants if $|\text{Image}(\theta_{n,e})| \sim_n q^{ep^n}$ for all $e \geq 1$.

Here, $a_e \sim_e b_e$ signify that a_e and b_e are positive integers such that a_e/b_e and b_e/a_e are bounded independently of e (but the bounds may depend on m). Likewise, $a_n \sim_n b_n$ signify that a_n and b_n are positive integers such that a_n/b_n and b_n/a_n are bounded independently of n (but the bounds may depend on e). Apart from our control theorems, the proof of Theorem C relies on global duality and global Euler characteristic formulae that the growth conditions on the localization maps are equivalent to criteria established by Greenberg (see Proposition 4.1)

Remark 1.1 We remind the reader that [8, Conjecture A], which generalizes [3, Conjecture A] (see also [2, Conjecture 1.2]), predicts that μ -invariants of U and V are always zero. Theorem C(ii) asserts that if the condition $|\text{Image}(\theta_{n,e})| \sim_n q^{ep^n}$ holds, then the μ -invariant of U vanishes if and only if that of V vanishes. Conversely, if the μ -invariants of these fine Selmer groups are zero, then the growth condition $|\text{Image}(\theta_{n,e})| \sim_n q^{ep^n}$ holds.

The following theorem gives sufficient conditions for $(H\text{-base}_F)$ to hold.

Theorem D (Theorem 5.1) *Let p be an odd prime and N a square-free integer coprime to p . Let $f \in S_k(\Gamma_0(N), \omega)$ be a newform with nebentypus character ω of conductor M . Let $0 \leq i \leq k$ be an integer. For a rational prime ℓ , let m_ℓ denote the order of ℓ in $(\mathbb{Z}/p\mathbb{Z})^\times$. Suppose that for each $\ell|N$ the following holds:*

- (i) $\ell \not\equiv 1 \pmod p$,
- (ii) *if $\ell|M$, then m_ℓ does not divide $(1 - k + i)$ or $(1 - i)$, and*

(iii) if $\ell \mid \frac{N}{M}$, then $\gcd(m_\ell, \phi(M)) = 1$ and m_ℓ does not divide k or $(k - 2)$.

Then, for all primes v of \mathbb{Q}_{cyc} that divide N , we have $H^0(\mathbb{Q}_{\text{cyc},v}, A_g(j))$ is finite for both $(g, j) = (f, i)$ and $(\bar{f}, k - i)$.

In Sect. 5.3, some explicit examples are computed satisfying the hypotheses of the above theorem.

For elliptic curves E/\mathbb{Q} , recall from [10, Problem 0.7] the following problem posed by Greenberg:

$$\text{Char}_\Lambda \text{Sel}_0(E/\mathbb{Q}_{\text{cyc}})^\vee \stackrel{?}{=} \left(\prod_{e_n \geq 1, n \geq 0} \Phi_n^{e_n - 1} \right). \tag{Gr}$$

Here, for $n \geq 1$,

$$\Phi_n = \frac{(1 + X)^{p^n} - 1}{(1 + X)^{p^{n-1}} - 1} \in \Lambda,$$

denotes the p^n -th cyclotomic polynomial in $1 + X$ and

$$e_n = \frac{\text{rank } E(L_n) - \text{rank } E(L_{n-1})}{p^{n-1}(p - 1)},$$

where L_n denotes the unique subextension of \mathbb{Q}_{cyc} such that $[L_n : \mathbb{Q}] = p^n$. When $n = 0$, we define $\Phi_0 = X$ and $e_0 = \text{rank } E(\mathbb{Q})$. The right-hand side of (Gr) is invariant under ι ; this suggests that we might expect there is a pseudo-isomorphism between $\text{Sel}_0(E/\mathbb{Q}_{\text{cyc}})$ and $\text{Sel}_0(E/\mathbb{Q}_{\text{cyc}})^\iota$. Recent results of Nakamura [14] on functional equations of Kato’s Euler systems suggest that the expectation may be reasonable. Therefore, one is tempted to conjecture that the growth of the image conditions given in Theorem C hold true.

2 Setup and notation

Fix an algebraic closure $\overline{\mathbb{Q}}$ of \mathbb{Q} . Then an algebraic extension of \mathbb{Q} is a subfield of this fixed algebraic closure, $\overline{\mathbb{Q}}$. Throughout, p denotes a fixed rational odd prime. Fix a finite set S of primes of \mathbb{Q} containing p , the primes dividing the level of the fixed modular form f , and the unique archimedean prime. Denote by \mathbb{Q}_S , the maximal algebraic extension of \mathbb{Q} unramified outside S . For every (possibly infinite) extension L of \mathbb{Q} contained in \mathbb{Q}_S , write $G_S(L) = \text{Gal}(\mathbb{Q}_S/L)$. Write $S(L)$ for the set of primes of L above S . If L is a finite extension of \mathbb{Q} and w is a place of L , we write L_w for its completion at w ; when L/\mathbb{Q} is infinite, it is the union of completions of all finite sub-extensions of L .

Definition 2.1 Let M be a \mathbb{Z}_p -module equipped with a continuous $G_S(\mathbb{Q})$ -action.

- (i) For any finite extension L/\mathbb{Q} and $j \in \{1, 2\}$, set

$$K_v^j(M/L) = \bigoplus_{w|v} H^j(L_w, M),$$

where the direct sum is taken over all primes w of L lying above v .

- (ii) For an infinite algebraic extension \mathcal{L}/\mathbb{Q} , we define $K_v^j(M/\mathcal{L})$ by taking the inductive limit of $K_v^j(M/L)$ over all finite extensions L/\mathbb{Q} contained in \mathcal{L} .
- (iii) Let L be an algebraic extension of \mathbb{Q} that is contained inside \mathbb{Q}_S , we define the **fine Selmer group** of M over L as

$$\text{Sel}_0(M/L) := \ker \left(H^1(G_S(\mathbb{Q}), M) \longrightarrow \bigoplus_{v \in S(L)} K_v^1(M/L) \right).$$

Since all primes are finitely decomposed in the cyclotomic \mathbb{Z}_p -extension, we will henceforth simplify notation and write $\bigoplus_{v \in S(\mathbb{Q}_{\text{cyc}})} H^1(\mathbb{Q}_{\text{cyc},v}, M)$ in place of $\bigoplus_{v \in S(\mathbb{Q}_{\text{cyc}})} K_v^1(M/L)$.

From now on, we fix a uniformizer ϖ of K . Recall from the introduction that Γ denotes the Galois group $\text{Gal}(\mathbb{Q}_{\text{cyc}}/\mathbb{Q})$ and $\Lambda = \mathcal{O}[[\Gamma]]$.

Definition 2.2 Let $F \in \Lambda$. Write Λ/F for the quotient module $\Lambda/\langle F \rangle$, where $\langle F \rangle$ denotes the Λ -ideal generated by F . Consider it as a $G_S(\mathbb{Q})$ -module via the projection $G_S(\mathbb{Q}) \longrightarrow \Gamma$ and Γ acts on Λ/F via the multiplication by identifying the elements of Γ with the group-like elements in Λ . For a $G_S(\mathbb{Q})$ -module M , define M_F to be the tensor product $M \otimes_{\mathcal{O}} \Lambda/F$ equipped with the diagonal action by $G_S(\mathbb{Q})$.

Note that action of $G_S(\mathbb{Q}_{\text{cyc}})$ on Λ/F is trivial.

Definition 2.3 Let $g = f$ or \bar{f} and $j \in \mathbb{Z}$. For any algebraic extension L/\mathbb{Q} contained in \mathbb{Q}_S and $F \in \Lambda$, the **F -twisted fine Selmer group** of $A_g(j)$ over L is defined as $\text{Sel}_0(A_g(j)_F/L)$. Similarly, we define the **F -twisted ϖ^e -fine Selmer group** of $A_g(j)$ over L to be $\text{Sel}_0(A_g(j)_F[\varpi^e]/L)$.

Let M be a finitely generated Λ -module, then there exists a pseudo-isomorphism

$$M \sim \Lambda^a \oplus \bigoplus_{i=1}^s \Lambda/\varpi^{\alpha_i} \oplus \bigoplus_{j=1}^t \bigoplus_{\ell=1}^{u_j} \Lambda/F_j^{\beta_{j,\ell}},$$

where $a, s, t \geq 0$, $\alpha_i, \beta_{j,\ell} \geq 1$ are integers, F_j 's are mutually coprime irreducible distinguished polynomials in Λ . Also, the pseudo-isomorphism is unique up to rearrangements of the direct summands. We write

$$M(\varpi^\infty) = \bigoplus_{i=1}^s \Lambda/\varpi^{\alpha_i},$$

and define the μ -invariant of M to be $\sum_{i=1}^s \alpha_i$. Given an irreducible distinguished polynomial $F \in \Lambda$, we write

$$M(F^\infty) = \begin{cases} \bigoplus_{\ell=1}^{u_j} \Lambda / F_j^{\beta_{j,\ell}} & \text{if } F = F_j \text{ for some } j, \\ 0 & \text{otherwise.} \end{cases}$$

The following hypothesis will be used whenever necessary throughout the article. **Hypothesis (H-base_F):** For all primes $v|N$, $H^0(\mathbb{Q}_v, A_g(j) \otimes_{\mathcal{O}} \Lambda/\mathcal{F})$ is finite for $(g, j, \mathcal{F}) = (f, i, F)$ and $(\bar{f}, k - i, F')$, where F is an irreducible distinguished polynomial in Λ .

The following stronger hypothesis, which we call (H-cyc), implies (H-base_F) for any F . **Hypothesis (H-cyc):** For all primes v of \mathbb{Q}_{cyc} that divide N , we have $H^0(\mathbb{Q}_{\text{cyc},v}, A_g(j))$ is finite for both $(g, j) = (f, i)$ and $(\bar{f}, k - i)$. Indeed, the above assertion follows from the observation that

$$\begin{aligned} H^0(\mathbb{Q}_v, A_g(j) \otimes_{\mathcal{O}} \Lambda/\mathcal{F}) &\subset H^0(\mathbb{Q}_{\text{cyc},v}, A_g(j) \otimes_{\mathcal{O}} \Lambda/\mathcal{F}) \\ &= H^0(\mathbb{Q}_{\text{cyc},v}, A_g(j)) \otimes_{\mathcal{O}} \Lambda/\mathcal{F}. \end{aligned}$$

This stronger hypothesis (H-cyc) is verified for certain explicit examples in §5.

3 Control theorems

In this section, we prove two control theorems required for the proof of our theorems. We fix an irreducible distinguished polynomial F and an integer $m \geq 1$.

3.1 First control theorem

Here, we prove a control theorem that allows us to go between the ϖ^e -fine Selmer groups of $A_g(j)$ and the ϖ^e -torsion subgroup of the fine Selmer group of $A_g(j)$.

Let G be a profinite group and M an \mathcal{O} -module equipped with a continuous G -action. The short exact sequence

$$0 \longrightarrow M[\varpi^e] \longrightarrow M \xrightarrow{\varpi^e} M \longrightarrow 0$$

induces the following short exact sequence in Galois cohomology for $j \geq 1$,

$$0 \longrightarrow H^{j-1}(G, M) / \varpi^e \longrightarrow H^j(G, M[\varpi^e]) \longrightarrow H^j(G, M) [\varpi^e] \longrightarrow 0, \quad (3.1)$$

which is a crucial ingredient in proving the first control theorem. We also need the following lemma.

Lemma 3.1 *Let $e \geq 1$ be an integer. Let N be a cofinitely generated \mathcal{O} -module. Then $|N/\varpi^e|$ is bounded independently of e .*

Proof Recall that K/\mathbb{Q}_p is a finite extension with ring of integers \mathcal{O} . We first write

$$N \simeq (K/\mathcal{O})^{d_0} \oplus N_{\text{finite}}, \quad \text{where } d_0 \geq 0.$$

Since K/\mathcal{O} is divisible, it follows that $(K/\mathcal{O})^{d_0}/\varpi^e = 0$. Therefore, we only need to study the finite part. Note that

$$N_{\text{finite}} \simeq \bigoplus_{i=1}^t \mathcal{O}/\varpi^{n_i} \quad \text{with } t \leq d, n_i \geq 1.$$

Therefore,

$$(\mathcal{O}/\varpi^{n_i})/\varpi^e \simeq \begin{cases} \mathcal{O}/\varpi^{n_i} & \text{if } e \geq n_i, \\ \mathcal{O}/\varpi^e & \text{if } e < n_i. \end{cases}$$

In either case, we have that $|(\mathcal{O}/\varpi^{n_i})/\varpi^e| \leq q^{n_i}$. The result follows. □

We now prove our first control theorem (see Theorem A).

Theorem 3.2 *Let $e \geq 1$ be fixed integers and M a cofinitely generated \mathcal{O} -module equipped with a continuous $G_S(\mathbb{Q})$ -action. Let \mathcal{F} be a subfield of \mathbb{Q}_{cyc} . Then the natural map*

$$r : \text{Sel}_0(M[\varpi^e]/\mathcal{F}) \longrightarrow \text{Sel}_0(M/\mathcal{F})[\varpi^e]$$

has finite kernel and cokernel with order bounded independently of e .

Proof We have the following commutative diagram with exact rows

$$\begin{CD} 0 @>>> \text{Sel}_0(M[\varpi^e]/\mathcal{F}) @>>> H^1(G_S(\mathcal{F}), M[\varpi^e]) @>>> \bigoplus_{v \in S(\mathcal{F})} H^1(\mathcal{F}_v, M[\varpi^e]) \\ @. @V r VV @V h VV @VV \gamma = \bigoplus \gamma_v V \\ 0 @>>> \text{Sel}_0(M/\mathcal{F})[\varpi^e] @>>> H^1(G_S(\mathcal{F}), M)[\varpi^e] @>>> \bigoplus_{v \in S(\mathcal{F})} H^1(\mathcal{F}_v, M)[\varpi^e], \end{CD}$$

where h (resp. γ_v) arises from the short exact sequence (3.1) with $j = 1$ and $G = G_S(\mathcal{F})$ (or $G = \text{Gal}(\overline{\mathcal{F}_v}/\mathcal{F}_v)$). These maps are surjective, and we have

$$\ker h = M^{G_{\mathcal{F}}}/\varpi^e \quad \text{and} \quad \ker \gamma = \bigoplus_{v \in S(\mathcal{F})} M^{G_{\mathcal{F}_v}}/\varpi^e.$$

Note that

$$\left| H^0(G, M) / \varpi^e \right| \leq \left| H^0(G, M) / \left(H^0(G, M) \right)_{\text{div}} \right|,$$

which is finite and independent of e . Furthermore, all primes of \mathbb{Q} are finitely decomposed in \mathbb{Q}_{cyc} . Therefore, both $\ker h$ and $\ker \gamma$ are finite and bounded independently of e . The result follows from the snake lemma. \square

3.2 Second control theorem

We now prove a control theorem which allows us to go between fine Selmer groups over \mathbb{Q}_{cyc} and L_n . We begin by proving several preliminary lemmas.

Lemma 3.3 *Let $M = A_f(i)_{F^m}$ or $A_{\bar{f}}(k-i)_{F^l, m}$. The group $H^0(\mathbb{Q}_p(\mu_{p^\infty}), M)$ is finite.*

Proof We only consider the case $M = A_f(i)_{F^m}$ since the other case can be proved similarly. By definition, we have

$$M = A_f \otimes_{\mathcal{O}} (\Lambda / F^m)(i).$$

As the Galois group $G_{\mathbb{Q}_p(\mu_{p^\infty})}$ acts trivially on $(\Lambda / F^m)(i)$, we have

$$H^0(\mathbb{Q}_p(\mu_{p^\infty}), M) = H^0(\mathbb{Q}_p(\mu_{p^\infty}), A_f) \otimes_{\mathcal{O}} (\Lambda / F^m)(i).$$

Therefore, it suffices to show that $H^0(\mathbb{Q}_p(\mu_{p^\infty}), A_f)$ is finite. By local Tate duality, we have

$$H^0(\mathbb{Q}_p(\mu_{p^\infty}), A_f)^\vee \cong H_{\text{Iw}}^2(\mathbb{Q}_p(\mu_{p^\infty}), T_{\bar{f}}(k)) = \varprojlim H^2(\mathbb{Q}_p(\mu_{p^n}), T_{\bar{f}}(k)).$$

Recall that we have assumed $p \nmid N$. Thus, by [9, Theorem 12.5(3)] we know that the localization of $H_{\text{Iw}}^2(\mathbb{Q}_p(\mu_{p^\infty}), T_{\bar{f}}(k))$ at a height-one prime that does not contain p is zero. In particular, as Λ -modules, we have a pseudo-isomorphism

$$H^0(\mathbb{Q}_p(\mu_{p^\infty}), A_f)^\vee \sim \bigoplus_{i=1}^s \Lambda / \varpi^{\alpha_i}$$

for some integers $s, \alpha_i \geq 0$. But $A_f \cong (K/\mathcal{O})^{\oplus 2}$ as an \mathcal{O} -module. Thus, $H^0(\mathbb{Q}_p(\mu_{p^\infty}), A_f)^\vee$ is an \mathcal{O} -module of rank at most 2. This forces $\alpha_i = 0$ for all i . In particular, $H^0(\mathbb{Q}_p(\mu_{p^\infty}), A_f)$ is a pseudo-null Λ -module as required. \square

Remark 3.4 Note that

$$H^0(\mathbb{Q}_{\text{cyc}}, M) \subset H^0(\mathbb{Q}_p(\mu_{p^\infty}), M).$$

Therefore, $H^0(\mathbb{Q}_{\text{cyc}}, M)$ is also finite.

Lemma 3.5 Hypothesis $(H\text{-base}_F)$ implies that both $H^0(\mathbb{Q}_v, A_f(i)_{F^m})$ and $H^0(\mathbb{Q}_v, A_{\bar{f}}(k-i)_{F^{v,m}})$ are finite for all $v|N$.

Proof When $m = 1$, this is clear. Suppose that $m > 1$, the short exact sequence

$$0 \longrightarrow F\Lambda/F^m \longrightarrow \Lambda/F^m \longrightarrow \Lambda/F \longrightarrow 0$$

gives rise to the following short exact sequence

$$0 \longrightarrow A_f(i)_{F^{m-1}} \xrightarrow{\times F} A_f(i)_{F^m} \longrightarrow A_f(i)_F \longrightarrow 0.$$

The left most injectivity follows from the \mathcal{O} -freeness of Λ/F . From this, we obtain the long exact sequence

$$0 \longrightarrow H^0(\mathbb{Q}_v, A_f(i)_{F^{m-1}}) \longrightarrow H^0(\mathbb{Q}_v, A_f(i)_{F^m}) \longrightarrow H^0(\mathbb{Q}_v, A_f(i)_F) \longrightarrow \dots$$

Therefore, the lemma follows from induction. □

Lemma 3.6 Let M be a cofinitely generated \mathcal{O} -module equipped with a continuous action of $G_S(\mathbb{Q})$. Let \mathcal{F} be either \mathbb{Q} or \mathbb{Q}_ℓ , where ℓ is a prime number dividing pN . Suppose that $\mathcal{F}_\infty/\mathcal{F}$ is the cyclotomic \mathbb{Z}_p -extension of \mathcal{F} and \mathcal{F}_n is the intermediate subfield of \mathcal{F}_∞ with $[\mathcal{F}_n : \mathcal{F}] = p^n$. Write $G_n = \text{Gal}(\mathcal{F}_\infty/\mathcal{F}_n)$ and $M(\mathcal{F}_\infty) = H^0(\mathcal{F}_\infty, M)$.

- (i) Let $e \geq 1$ be a fixed integer. Then $H^1(G_n, M[\varpi^e](\mathcal{F}_\infty))$ is finite and bounded as n varies.
- (ii) Suppose that $A_f(i)_{F^m}$ or $A_{\bar{f}}(i)_{F^{v,m}}$ and that $(H\text{-base}_F)$ holds. Then $H^1(G_0, M(\mathcal{F}_\infty))$ is finite.

Proof With our notation, $\mathcal{F}_0 = \mathcal{F}$ and $G_0 = \text{Gal}(\mathcal{F}_\infty/\mathcal{F})$.

- (i) As $M[\varpi^e]$ is finite, $M[\varpi^e](\mathcal{F}_\infty)$ is also finite. Since G_n is pro-cyclic, we have

$$H^1(G_n, M[\varpi^e](\mathcal{F}_\infty)) \cong H_0(G_n, M[\varpi^e](\mathcal{F}_\infty)).$$

This is finite and bounded by the order of $M[\varpi^e](\mathcal{F}_\infty)$, which is independent of n , as required.

- (ii) Consider the exact sequence

$$0 \longrightarrow H^0(G_0, M(\mathcal{F}_\infty)) \longrightarrow M(\mathcal{F}_\infty) \xrightarrow{\gamma-1} M(\mathcal{F}_\infty) \longrightarrow H_0(G_0, M(\mathcal{F}_\infty)) \longrightarrow 0,$$

where γ is a topological generator of G_0 . Since $H^0(G_0, M(\mathcal{F}_\infty)) = H^0(\mathcal{F}, M)$ is finite by Lemmas 3.3 and 3.5, we have

$$M(\mathcal{F}_\infty)_{\text{div}} \subset (\gamma - 1)M(\mathcal{F}_\infty).$$

Thus, $H^1(G_0, M(\mathcal{F}_\infty)) \cong H_0(G_0, M(\mathcal{F}_\infty))$ is bounded by $M(\mathcal{F}_\infty)/M(\mathcal{F}_\infty)_{\text{div}}$, which is finite. This concludes the proof. □

We can now prove our second control theorem (see Theorem B).

Theorem 3.7 *Let M be a cofinitely generated \mathcal{O} -module equipped with a continuous action of $G_S(\mathbb{Q})$. Let $n \geq 0$ be an integer.*

(i) *Let $e \geq 1$ be an integer. Then the kernel and cokernel of the restriction map*

$$r_n : \text{Sel}_0(M[\varpi^e]/L_n) \longrightarrow \text{Sel}_0(M[\varpi^e]/\mathbb{Q}_{\text{cyc}})^{\Gamma_n}$$

are finite and bounded independently of n .

(ii) *Let F be a fixed irreducible distinguished polynomial and $m \geq 1$ an integer. Suppose that $M = A_f(i)_{F^m}$ or $A_{\overline{F}}(k-i)_{F^{t,m}}$ and that $(H\text{-base}_F)$ holds. Then, the kernel and cokernel of the restriction map*

$$r : \text{Sel}_0(M/\mathbb{Q}) \longrightarrow \text{Sel}_0(M/\mathbb{Q}_{\text{cyc}})^{\Gamma}$$

are finite.

Proof Let $\mathcal{M} = M$ or $M[\varpi^e]$. Consider the diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & \text{Sel}_0(\mathcal{M}/L_n) & \longrightarrow & H^1(G_S(L_n), \mathcal{M}) & \longrightarrow & \bigoplus_{v \in S(L_n)} H^1(L_{n,v}, \mathcal{M}) \\ & & \downarrow r_n & & \downarrow h_n & & \downarrow \gamma_n \\ 0 & \longrightarrow & \text{Sel}_0(\mathcal{M}/\mathbb{Q}_{\text{cyc}})^{\Gamma_n} & \longrightarrow & H^1(G_S(\mathbb{Q}_{\text{cyc}}), \mathcal{M})^{\Gamma_n} & \longrightarrow & \bigoplus_{v \in S(\mathbb{Q}_{\text{cyc}})} H^1(\mathbb{Q}_{\text{cyc},v}, \mathcal{M})^{\Gamma_n} \end{array}$$

The vertical maps h_n and γ_n are the natural restriction maps. These induce the left vertical map. By inflation-restriction, first observe that both h_n and γ_n are surjective since Γ has p -cohomological dimension 1. By the inflation-restriction exact sequence, we know that

$$\ker h_n = H^1(\Gamma_n, \mathcal{M}(\mathbb{Q}_{\text{cyc}})) \quad \text{and} \quad \ker \gamma_n = \bigoplus_v H^1(\Gamma_{n,v}, \mathcal{M}(\mathbb{Q}_{\text{cyc},v})),$$

where $\Gamma_{n,v} = \text{Gal}(\mathbb{Q}_{\text{cyc},v}/\mathbb{Q}_{n,v})$. Therefore, in the setting of (i), by Lemma 3.6(i) both $\ker h_n$ and $\ker \gamma_n$ are finite and bounded independently of n . In the setting of (ii), by Lemma 3.6(ii) both $\ker h_0$ and $\ker \gamma_0$ are finite. The result follows by an application of the snake lemma. □

Remark 3.8 Part (ii) of Theorem B is utilized in the proof of Theorem C(i), whereas part (i) is employed to prove Theorem C(ii). Note that we do not require the twist by Λ/F^m (or $\Lambda/F^{t,m}$) when we apply part (i) in the proof of Theorem C(ii).

4 Proof of Theorem C

We review the criteria to establish a pseudo-isomorphism between two cofinitely generated Λ -modules developed by Greenberg.

Proposition 4.1 *Let U and V be two finitely generated torsion Λ -modules.*

- (1) *Let $F \in \Lambda$ be an irreducible distinguished polynomial. Then for all integers $m \geq 0$, $\text{corank}_{\mathbb{Z}_p}((U^\vee)_{F^m})^\Gamma = \text{corank}_{\mathbb{Z}_p}((V^\vee)_{F^m})^\Gamma$ if and only if $U(F^\infty) = V(F^\infty)$.*
- (2) *For every integer $e \geq 0$, the quotient $| (U/\varpi^e)_{\Gamma_n} | / | (V/\varpi^e)_{\Gamma_n} |$ is bounded as n varies if and only if $U(\varpi^\infty) = V(\varpi^\infty)$.*

Proof This result is essentially due to Greenberg [7]. The proofs follow from the arguments given in Lemmas 2.1, 2.2 and Proposition 2.3 in [1, §2.1]. □

For our purposes, the proposition will be applied to $U = \text{Sel}_0(A_f(i)/\mathbb{Q}_{\text{cyc}})^\vee$ and $V = \text{Sel}_0(A_{\bar{f}}(k-i)/\mathbb{Q}_{\text{cyc}})^{\vee,t}$.

Let us first introduce some notation. Let e be a fixed positive integer. Let \mathcal{M} denote either $A_f(i)_{F^m}[\varpi^e]$ or $A_f(i)[\varpi^e]$, both of which are finite Galois modules of p -power order. The Cartier dual $\mathcal{M}^\dagger := \text{Hom}(\mathcal{M}, \mu_{p^\infty})$ is $A_{\bar{f}}(k-i)_{F^{\iota,m}}[\varpi^e]$ (resp. $A_{\bar{f}}(k-i)[\varpi^e]$). We check this for $\mathcal{M} = A_f(i)[\varpi^e]$ (checking the claim for the other module is similar):

$$\begin{aligned} (A_f(i)[\varpi^e])^\dagger &= (A_f(i))^\dagger / \varpi^e \\ &= T_{\bar{f}}(k-i) / \varpi^e \\ &= A_{\bar{f}}(k-i)[\varpi^e]. \end{aligned}$$

Let \mathcal{K} be either \mathbb{Q} or L_n . For $j = 1, 2$, we define the maps

$$\begin{aligned} \lambda_{\mathcal{M}}^{(j)} : H^j(G_S(\mathcal{K}), \mathcal{M}) &\longrightarrow \bigoplus_{v \in S} H^j(\mathcal{K}_v, \mathcal{M}) \\ \lambda_{\mathcal{M}^\dagger}^{(j)} : H^j(G_S(\mathcal{K}), \mathcal{M}^\dagger) &\longrightarrow \bigoplus_{v \in S} H^j(\mathcal{K}_v, \mathcal{M}^\dagger). \end{aligned}$$

Set

$$\begin{aligned} K_j &= K_j(\mathcal{M}) = \ker(\lambda_{\mathcal{M}}^{(j)}), & K_j^\dagger &= K_j(\mathcal{M}^\dagger) = \ker(\lambda_{\mathcal{M}^\dagger}^{(j)}), \\ G_j &= G_j(\mathcal{M}) = \text{Image}(\lambda_{\mathcal{M}}^{(j)}), & G_j^\dagger &= G_j(\mathcal{M}^\dagger) = \text{Image}(\lambda_{\mathcal{M}^\dagger}^{(j)}). \end{aligned}$$

We note that K_1 (resp. K_1^\dagger) is the fine Selmer group of \mathcal{M} (resp. \mathcal{M}^\dagger) over \mathcal{K} .

Lemma 4.2 *We have the equality*

$$\frac{|K_1^\dagger|}{|K_1|} = \frac{|G_1| \cdot \chi_{\text{glob}}(\mathcal{K}, \mathcal{M})}{|H^0(G_S(\mathcal{K}), \mathcal{M})| \cdot |G_2|}.$$

Proof By global duality (see [19, Theorem 3.1(a)]), we have

$$|K_1^\dagger| = |K_2| = \frac{|H^2(G_S(\mathcal{K}), \mathcal{M})|}{|G_2|}.$$

The global Euler characteristic formula states that

$$\chi_{\text{glob}}(\mathcal{K}, \mathcal{M}) = \prod_{i=0}^2 |H^i(G_S(\mathcal{K}), \mathcal{M})|^{(-1)^i}.$$

This allows us to deduce

$$\begin{aligned} |K_1^\dagger| &= \frac{|H^1(G_S(\mathcal{K}), \mathcal{M})| \cdot \chi_{\text{glob}}(\mathcal{M})}{|H^0(G_S(\mathcal{K}), \mathcal{M})| \cdot |G_2|} \\ &= \frac{|K_1| \cdot |G_1| \cdot \chi_{\text{glob}}(\mathcal{M})}{|H^0(G_S(\mathcal{K}), \mathcal{M})| \cdot |G_2|} \end{aligned}$$

as required. □

Proof of Theorem C(i) Fix an integer $m \geq 1$ and take $\mathcal{M} = A_f(i)_{F^m}[\varpi^e]$ and $\mathcal{K} = \mathbb{Q}$. We work under the hypotheses (H-base_F).

Lemma 4.3 *With the notation of Lemma 4.2,*

$$\frac{|K_1^\dagger|}{|K_1|} \sim_e |\text{Image}(\theta_{F,m,e})| \cdot \chi_{\text{glob}}(\mathbb{Q}, \mathcal{M}).$$

Proof By Lemma 3.3, we know that $|H^0(G_S(\mathcal{K}), \mathcal{M})| \sim_e 1$ since

$$H^0(G_S(\mathbb{Q}), \mathcal{M}) \subset H^0(G_S(\mathbb{Q}_{\text{cyc}}, A_f) \otimes_{\mathcal{O}} \Lambda/F^m(i)).$$

To bound $|G_2|$, it is enough to observe that

$$G_2 \subset \bigoplus_{v \in S} H^2(\mathbb{Q}_v, \mathcal{M}) \cong \bigoplus_{v \in S} H^0(\mathbb{Q}_v, \mathcal{M}^\dagger)^\vee,$$

where the isomorphism is the local Tate duality. But

$$H^0(\mathbb{Q}_v, \mathcal{M}^\dagger) \subset H^0(\mathbb{Q}_v, A_{\bar{f}}(k-i)_{F^l,m}),$$

which is finite for all v by Lemmas 3.3 and 3.5. Therefore, $|G_2| \sim_e 1$.

It remains to compare $|G_1|$ with $|\text{Image}(\theta_{F,m,e})|$. Here, $\theta_{F,m,e}$ is the composition

$$H^1(G_S(\mathbb{Q}), \mathcal{M}) \xrightarrow{\lambda_{\mathcal{M}}^{(1)}} \bigoplus_{v \in S} H^1(\mathbb{Q}_v, \mathcal{M}) \longrightarrow H^1(\mathbb{Q}_p, \mathcal{M}),$$

where the last arrow is given by the projection map. Therefore, it is enough to bound $H^1(\mathbb{Q}_v, \mathcal{M})$ for $v|N$. Since \mathcal{M} is a p -group, the local Euler characteristic formula gives

$$\begin{aligned} |H^1(\mathbb{Q}_v, \mathcal{M})| &= |H^0(\mathbb{Q}_v, \mathcal{M})| |H^2(\mathbb{Q}_v, \mathcal{M})| \\ &\leq |H^0(\mathbb{Q}_v, A_f(i)_{F^m})| |H^0(\mathbb{Q}_v, A_{\bar{F}}(k-i)_{F^{\iota,m}})|, \end{aligned}$$

which is bounded independently of e by Lemma 3.5 under (H-base $_F$). The result now follows. □

Recall from Proposition 4.1(1) that we need to show

$$\text{corank}_{\mathbb{Z}_p} \text{Sel}_0(A_f(i)_{F^m}/\mathbb{Q}_{\text{cyc}})^\Gamma = \text{corank}_{\mathbb{Z}_p} \text{Sel}_0(A_{\bar{F}}(k-i)_{F^{\iota,m}}/\mathbb{Q}_{\text{cyc}})^\Gamma$$

is equivalent to $\text{Image}(\theta_{F,m,e}) \sim_e q^{e \deg(F^m)}$. By the second control theorem (see Theorem B(ii)) this is equivalent to show

$$\text{corank}_{\mathbb{Z}_p} \text{Sel}_0(A_f(i)_{F^m}/\mathbb{Q}) = \text{corank}_{\mathbb{Z}_p} \text{Sel}_0(A_{\bar{F}}(k-i)_{F^{\iota,m}}/\mathbb{Q})$$

is equivalent to $\text{Image}(\theta_{F,m,e}) \sim_e q^{e \deg(F^m)}$. It follows from the Structure Theorem of cofinitely generated \mathcal{O} -modules that

$$|\text{Sel}_0(A_f(i)_{F^m}/\mathbb{Q})[\varpi^e]| \sim_e |\text{Sel}_0(A_{\bar{F}}(k-i)_{F^{\iota,m}}/\mathbb{Q})[\varpi^e]|$$

is equivalent to $\text{Image}(\theta_{F,m,e}) \sim_e q^{e \deg(F^m)}$. On applying Theorem A (with $n = 0$ and e varying), it is enough to show that

$$|\text{Sel}_0(A_f(i)_{F^m}[\varpi^e]/\mathbb{Q})| \sim_e |\text{Sel}_0(A_{\bar{F}}(k-i)_{F^{\iota,m}}[\varpi^e]/\mathbb{Q})| \tag{4.1}$$

is equivalent to $\text{Image}(\theta_{F,m,e}) \sim_e q^{e \deg(F^m)}$. Since \mathbb{Q} is a totally real field, the global Euler characteristic formula tells us that

$$\chi_{\text{glob}}(\mathbb{Q}, \mathcal{M}) = \frac{1}{|\mathcal{M}^-|} = \frac{1}{q^{e \deg(F^m)}},$$

where \mathcal{M}^- denotes the -1 -eigensubspace of the complex conjugation in \mathcal{M} . On combining this with Lemma 4.3, we deduce (4.1), as required. This concludes the proof of Theorem C(i). \square

4.1 Proof of Theorem C(ii)

Fix an integer $e \geq 1$, set $\mathcal{M} = A_f(i)[\varpi^e]$, and $\mathcal{K} = L_n$. We have the following analog of Lemma 4.3.

Lemma 4.4 *With the notation of Lemma 4.2,*

$$\frac{|K_1^\dagger|}{|K_1|} \sim_n |\text{Image}(\theta_{n,e})| \cdot \chi_{\text{glob}}(L_n, \mathcal{M}).$$

Proof By Lemma 3.3, we know that $|H^0(G_S(\mathcal{K}), \mathcal{M})| \sim_n 1$ since

$$H^0(G_S(L_n), \mathcal{M}) \subset H^0(G_S(\mathbb{Q}_{\text{cyc}}), A_f(i)).$$

To bound $|G_2|$, observe that

$$G_2 \subset \bigoplus_{v \in S(L_n)} H^2(L_{n,v}, \mathcal{M}) \cong \bigoplus_{v \in S(L_n)} H^0(L_{n,v}, \mathcal{M}^\dagger)^\vee$$

by local Tate duality. But $H^0(L_{n,v}, \mathcal{M}^\dagger)$ has at most q^{2e} elements and the number of primes above S are bounded as n varies. Therefore, $|G_2| \sim_n 1$.

It remains to compare $|G_1|$ with $|\text{Image}(\theta_{n,e})|$. Note that $\theta_{n,e}$ is the composition

$$H^1(G_S(F_n), \mathcal{M}) \xrightarrow{\lambda_{\mathcal{M}}^{(1)}} \bigoplus_{v \in S(L_n)} H^1(L_{n,v}, \mathcal{M}) \longrightarrow H^1(L_{n,p}, \mathcal{M}),$$

where the last arrow is given by the projection map. Since \mathcal{M} is a p -group, for $v \nmid p$, the local Euler characteristic formula gives

$$\begin{aligned} |H^1(L_{n,v}, \mathcal{M})| &= |H^0(L_{n,v}, \mathcal{M})| |H^2(L_{n,v}, \mathcal{M})| \\ &= |H^0(L_{n,v}, \mathcal{M})| |H^0(L_{n,v}, \mathcal{M}^\dagger)|, \end{aligned}$$

which is bounded independently of q^{4e} . Therefore, the result follows. \square

Recall from Proposition 4.1(2) that we need to show

$$\left| (\text{Sel}_0(A_f(i)/\mathbb{Q}_{\text{cyc}})[\varpi^e])^{\Gamma_n} \right| \sim_n \left| (\text{Sel}_0(A_{\overline{f}}(k-i)/\mathbb{Q}_{\text{cyc}})[\varpi^e])^{\Gamma_n} \right|$$

if and only if $|\text{Image}(\theta_{n,e})| \sim_n q^{ep^n}$. In view of Theorem A (with $\mathcal{F} = \mathbb{Q}_{\text{cyc}}$) and Theorem B(i)), this amounts to showing

$$|\text{Sel}_0(A_f(i)[\varpi^e]/L_n)| \sim_n |\text{Sel}_0(A_{\bar{f}}(k-i)[\varpi^e]/L_n)|, \tag{4.2}$$

if and only if $|\text{Image}(\theta_{n,e})| \sim_n q^{ep^n}$. The global Euler characteristic formula tells us that

$$\chi_{\text{glob}}(L_n, \mathcal{M}) = \frac{1}{|\mathcal{M}^-|} = \frac{1}{q^{ep^n}}$$

since L_n is a totally real field. Therefore, from Lemma 4.4 we deduce that (4.2) holds if and only if the required growth condition is satisfied. This concludes the proof of Theorem C(ii). \square

5 Computing invariants of local Galois representations

We write

$$\rho_f : G_{\mathbb{Q}} \rightarrow \text{GL}_2(K),$$

for the representation realized by V_f . Recall that we are using the geometric normalization, so that the determinant of ρ_f is given by $\epsilon_p^{1-k}\omega^{-1}$, where ϵ_p is the p -cyclotomic character, and ω is the nebentypus character of f of conductor M . We will write $\rho_{f,i} := \epsilon_p^i \otimes \rho_f$ for the i -th Tate twist of ρ_f .

For any rational prime ℓ , write \mathbb{Q}_{ℓ} for the completion of \mathbb{Q} at ℓ , and write $\mathbb{Q}_{\ell}^{\infty}$ for the cyclotomic \mathbb{Z}_p -extension of \mathbb{Q}_{ℓ} (which we may identify with $\mathbb{Q}_{\text{cyc},v}$, where v is a place of \mathbb{Q}_{cyc} lying above ℓ). We denote by G_{ℓ} and G_{ℓ}^{∞} their respective absolute Galois groups. In this section, we explain how to verify (in some simple cases) the following condition: **(H-cyc')** For all primes $\ell|N$, we have $H^0(\mathbb{Q}_{\ell}^{\infty}, \rho_{g,j}) = 0$ for both $(g, j) = (f, i)$ and $(\bar{f}, k - i)$.

Note that (H-cyc') is equivalent to (H-cyc) (since a nontrivial subspace in the K -vector space $H^0(\mathbb{Q}_{\ell}^{\infty}, \rho_{g,j})$ gives an infinite divisible group inside $H^0(\mathbb{Q}_{\ell}^{\infty}, A_g(j))$, and vice versa). The purpose of this section is to show that (H-cyc) is not too strong a hypothesis.

When referring to this hypothesis, we will often just refer to the pair (f, i) , which then determines the other pair $(\bar{f}, k - i)$.

Rather than give a complete study of (H-cyc'), we seek only to illustrate that it does hold quite often, and that in some situations it can be verified easily. To this end, we make the additional simplifying assumptions that f is a newform and that N is square-free. (These assumptions simplify the classification of the local Galois representations $\rho_{f,i}|_{G_{\ell}}$ via the local Langlands correspondence by eliminating the possibility of supersingular representations.)

Let ϕ denote the Euler totient function. We aim to prove the following result.

Theorem 5.1 *Let p be an odd prime and N be a square-free integer coprime to p . Let $f \in S_k(\Gamma_0(N), \omega)$ be a newform with nebentypus character ω of conductor M . Let $0 \leq i \leq k$ be an integer. For a rational prime ℓ , let m_ℓ denote the order of ℓ in $(\mathbb{Z}/p\mathbb{Z})^\times$. Suppose that for each $\ell|N$ the following holds:*

- (i) $\ell \not\equiv 1 \pmod{p}$,
- (ii) if $\ell|M$, then m_ℓ does not divide $(1 - k + i)$ or $(1 - i)$, and
- (iii) if $\ell|\frac{N}{M}$, then $\gcd(m_\ell, \phi(M)) = 1$ and m_ℓ does not divide k or $(k - 2)$.

Then (H-cyc') is satisfied.

Proof Under these assumptions, the fact that $H^0(\mathbb{Q}_\ell^\infty, \rho_{f,i}) = 0$ and $H^0(\mathbb{Q}_\ell^\infty, \rho_{\bar{f},k-i}) = 0$ for each $\ell|N$ follows from Propositions 5.6 and 5.7 below. \square

Remark 5.2 If ℓ has large order in $(\mathbb{Z}/p\mathbb{Z})^\times$ and $p \gg 3Mk$, then all three conditions will be met (except for possibly when $k = 2$ or $i = 1$). In fact, since the value of m_ℓ is related to the splitting behavior of ℓ in $\mathbb{Q}(\mu_p)$, the Chebotarev density theorem implies that a positive density of primes p can be used.

Remark 5.3 We emphasize that Theorem 5.1 only gives *sufficient* conditions for (H-cyc') to hold. We certainly do not expect all of the assumptions herein, especially the square-free level hypothesis, to be necessary. In any case, examples which can be verified using Theorem 5.1 abound, and we write down a few concrete examples at the end. It is easy to find many more using a computer algebra system such as SageMath [18].

5.1 A note on the cyclotomic character over \mathbb{Q}_ℓ^∞

Fix an odd prime p and a prime $\ell \neq p$. We are interested in the absolute Galois group of the field \mathbb{Q}_ℓ^∞ , which is the cyclotomic \mathbb{Z}_p -extension of \mathbb{Q}_ℓ . Let us make the following elementary observation.

Lemma 5.4 *If $\ell \not\equiv 1 \pmod{p}$, then \mathbb{Q}_ℓ^∞ contains no p -power roots of unity.*

Proof Since $\ell \neq p$, the extension $\mathbb{Q}_\ell^\infty/\mathbb{Q}_\ell$ is unramified, so the corresponding residue field is $\mathbf{F} = \bigcup_{n \geq 1} \mathbb{F}_{\ell p^n}$. Again since $\ell \neq p$, the p -power roots of unity in \mathbb{Q}_ℓ^∞ map isomorphically onto the p -power roots of unity in \mathbf{F} under the natural reduction map. But for each n , the only roots of unity in $\mathbb{F}_{\ell p^n}$ have order dividing $\ell^{p^n} - 1$. By Fermat's little theorem, $\ell^{p^n} \equiv \ell \pmod{p}$, so our assumption that $\ell \not\equiv 1 \pmod{p}$ ensures that p does not divide $\ell^{p^n} - 1$ for any n , which completes the proof. \square

An immediate corollary is that $\epsilon_p|_{G_\ell^\infty}$ is nontrivial, but since ϵ_p does become trivial over $\mathbb{Q}_\ell(\mu_{p^\infty})$, we see that $\epsilon_p|_{G_\ell^\infty}$ has finite order. More precisely, we have the following lemma.

Lemma 5.5 *Let m_ℓ denote the order of ℓ in $(\mathbb{Z}/p\mathbb{Z})^\times$. The restriction $\epsilon_p|_{G_\ell^\infty}$ of the p -cyclotomic character to \mathbb{Q}_ℓ^∞ has order m_ℓ .*

Proof From the construction of the cyclotomic \mathbb{Z}_p -extension \mathbb{Q}_ℓ^∞ and the fact that it is unramified over \mathbb{Q}_ℓ , we see that

$$[\mathbb{Q}_\ell(\mu_{p^\infty}) : \mathbb{Q}_\ell^\infty] = [\mathbb{F}_\ell(\mu_p) : \mathbb{F}_\ell] = m_\ell.$$

Since ϵ_p generates $\text{Gal}(\mathbb{Q}_\ell(\mu_{p^\infty})/\mathbb{Q}_\ell^\infty)$, this completes the proof. □

In the sections that follow, we will write I_ℓ for the inertia group inside G_ℓ . For F/\mathbb{Q}_ℓ a local field with absolute Galois group G_F , we will often view a character $\chi : G_F \rightarrow K^\times$ as a character $\chi : F^\times \rightarrow K^\times$ via the dense injection $F^\times \hookrightarrow G_F$ of local class field theory.

5.2 Local descriptions of Galois representations

To check (H-cyc'), it is necessary to understand the restriction of ρ_f to the decomposition group $G_\ell \subset G_{\mathbb{Q}}$ for each prime $\ell|N$. (Note that since $p \nmid N$, we always have $\ell \neq p$.) The local Langlands correspondence for $n = 2$ allows us to determine these restrictions explicitly. We will work entirely on the Galois side and make little mention of the automorphic story. Nevertheless, it is the classification on the automorphic side which permits the explicit descriptions of our local Galois representations. The standard reference for this material is Diamond–Im [6, §11], and a nicely-written modern treatment can be found in Loeffler–Weinstein [13], but note that both of these references use the arithmetic normalization (i.e., the Hodge–Tate weights of V_f are 0 and $k - 1$). The geometric normalization that we are using is also used in a paper of Weston [20, §5].

5.2.1 A few notes on our strategy

We will use two facts to simplify our computations. First, we will consider the base change of each local representation to the algebraic closure \bar{K} or $\bar{K}_{\mathfrak{p}}$ for $\mathfrak{p} | p$ a prime of K above p , since the existence of eigenvectors for ρ_f with K -rational eigenvalues is invariant under base change. (Base-change also preserves principal series and twist of Steinberg representations.)

Second, it suffices to study the semisimplification of each local representation, since

$$\dim_K H^0(G_\ell^\infty, \rho_f) \leq \dim_K H^0(G_\ell^\infty, \rho_f^{\text{ss}}). \tag{5.1}$$

Recall that f is of square-free level N , with nebentypus character ω of modulus M . Our computations are divided into two cases, depending on whether $\ell|M$ or $\ell \nmid \frac{N}{M}$.

5.2.2 Case $\ell|M$

Suppose $\ell|M$, so that the nebentypus character ω is ramified at ℓ . In this case, the local representation corresponds to a principal series representation $\pi(\chi_1, \chi_2)$ associated to

two continuous characters $\chi_i : G_\ell \rightarrow \overline{K}$, where χ_1 is ramified and χ_2 is unramified. The semisimplification of the associated Galois representation then satisfies

$$\rho_f|_{G_\ell}^{\text{ss}} \otimes \overline{K} \simeq \chi_1 \oplus \chi_2. \tag{5.2}$$

Proposition 5.6 *Let $f \in S_k(\Gamma_1(N), \omega)$ be a newform of square-free level, let m_ℓ denote the order of ℓ in $(\mathbb{Z}/p\mathbb{Z})^\times$. Suppose $\ell \not\equiv 1 \pmod p$ and $\ell|M$. If $m_\ell \nmid (1-k+i)$, then $H^0(\mathbb{Q}_\ell^\infty, \rho_{f,i}) = 0$.*

Proof By (5.1) and (5.2), it suffices to check whether $\epsilon_p^i \chi_1$ and $\epsilon_p^i \chi_2$ are both nontrivial over \mathbb{Q}_ℓ^∞ .

Let us first consider the case $i = 0$. In light of (5.2), upon taking the determinant of ρ_f we have the identity

$$\chi_1 \chi_2|_{G_\ell^\infty} = \epsilon^{1-k} \omega^{-1}|_{G_\ell^\infty}.$$

Since χ_1 is ramified and χ_2 is unramified, we must have

$$\chi_2|_{G_\ell^\infty} = \epsilon_p^{1-k}|_{G_\ell^\infty},$$

so by Lemma 5.5, this is nontrivial provided $m_\ell \nmid 1 - k$.

Similarly, since both χ_1 and ω are ramified, we must have

$$\chi_1|_{I_\ell} = \omega^{-1}|_{I_\ell}$$

is nontrivial. Since $\mathbb{Q}_\ell^\infty/\mathbb{Q}_\ell$ is unramified, we have $\chi_1|_{G_\ell^\infty}$ is nontrivial as desired.

Now suppose we twist χ_1 and χ_2 by ϵ_p^i . Since χ_1 is ramified and ϵ_p is unramified, their product is nontrivial no matter the value of i . On the other hand,

$$\epsilon_p^i \chi_2|_{G_\ell^\infty} = \epsilon_p^{1-k+i}|_{G_\ell^\infty},$$

so this is nontrivial provided m_ℓ does not divide $1 - k + i$. □

5.2.3 Case $\ell | \frac{N}{M}$

Recall that ω has conductor M . Now suppose $\ell | \frac{N}{M}$, so that ω is unramified at ℓ and the local representation corresponds to a special (twist of Steinberg) representation. This translates on the Galois side to

$$\rho_f|_{G_\ell} \otimes \overline{K}_\mathfrak{p} \simeq \begin{pmatrix} \epsilon_p \chi & * \\ 0 & \chi \end{pmatrix} \tag{5.3}$$

where $\chi : G_\ell \rightarrow \overline{K}^\times$ is an unramified character.

We point out that the following result depends only on the weight of the modular form and not on the specific twist.

Proposition 5.7 Let $f \in S_k(\Gamma_1(N), \omega)$ be newform of square-free level. Suppose $\ell \not\equiv 1 \pmod p$, and let m_ℓ denote the order of ℓ in $(\mathbb{Z}/p\mathbb{Z})^\times$. If $\ell | \frac{N}{M}$, assume that $\gcd(m_\ell, \phi(M)) = 1$ and $m_\ell \nmid k(k-2)$. Then $H^0(\mathbb{Q}_\ell^\infty, \rho_{f,i}) = 0$.

Proof Just as in the proof of Proposition 5.6, it suffices to show that neither $\epsilon_p^{i+1}\chi$ or $\epsilon_p^i\chi$ is trivial when restricted to G_ℓ^∞ . Note that by Lemma 5.5, at most one of these characters can be trivial. Assume that one of them is, and suppose $\epsilon_p^j\chi$ is nontrivial where $\{j, j'\} = \{i, i+1\}$. Upon restricting to G_ℓ^∞ , the determinant then gives us

$$\epsilon_p^j\chi|_{G_\ell^\infty} = \epsilon_p^{1-k}\omega|_{G_\ell^\infty}.$$

On the other hand, our assumption that $\epsilon_p^{j'}\chi|_{G_\ell^\infty}$ is trivial implies $\chi|_{G_\ell^\infty} = \epsilon_p^{-j'}|_{G_\ell^\infty}$, so combining these yields

$$1 = \epsilon_p^{1-k-j+j'}\omega|_{G_\ell^\infty} = \epsilon_p^t\omega|_{G_\ell^\infty},$$

for $t \in \{-k, 2-k\}$. Since $\gcd(m_\ell, \phi(M)) = 1$, this implies $\omega|_{G_\ell^\infty} = 1$ and $\epsilon_p^t|_{G_\ell^\infty} = 1$. But this is only possible if $m_\ell | t$ by Lemma 5.5. □

5.3 Examples

In this final section, we give a few explicit examples of the application of Theorem 5.1. These examples were all found using SageMath [18].

Example 5.8 Let f be the newform of weight 2 and level 13 whose Fourier coefficients live in $\mathbb{Q}(\sqrt{-3})$, and whose q -expansion begins

$$f = q + (-1 - \zeta_6)q^2 + (-2 + 2\zeta_6)q^3 + \zeta_6q^4 + (1 - 2\zeta_6)q^5 + \dots,$$

where ζ_6 is a primitive 6-th root of unity. In particular, f and \bar{f} are distinct. The nebentypus character of f has conductor 13, so condition (iii) of Proposition 5.1 is irrelevant. Thus, (f, i) and $(\bar{f}, k-i)$ satisfy (H-cyc') if one chooses a prime p such that

- (1) $p \geq 5$, so that $13 \not\equiv 1 \pmod p$,
- (2) the order of 13 in $(\mathbb{Z}/p\mathbb{Z})^\times$ does not divide $(1-i)$

For instance, this happens for $p = 5$ and $i \not\equiv 1 \pmod 4$, and for $p = 7$ with $i \equiv 0 \pmod 2$.

Example 5.9 Let f be the unique newform of weight 4 and level 11, with q -expansion beginning

$$f = q + (1 + \beta)q^2 + (-1 - 4\beta)q^3 + (-4 + 2\beta)q^4 + (1 + 8\beta)q^5 + \dots,$$

where $\beta = \sqrt{3}$. This form has trivial nebentypus, so condition (ii) of Proposition 5.1 is irrelevant, and $\phi(M) = 1$, so it is only necessary to pick $p > 5$, $p \neq 11$ such that $m_{11} \nmid 4$, and then any twist i can be chosen.

Since $11^4 = 14641$, one can quickly check using Sage that the only primes for which the hypotheses of Theorem 5.1 are not satisfied are 2, 3, 5, 11, and 61.

Example 5.10 Let f be the newform of weight 4 and level 10 with nontrivial nebentypus character ω of conductor 5 with q -expansion that begins

$$f = q + 2\zeta q^2 - 2\zeta q^3 - q^4 + (-5 - 10\zeta)q^5 + \dots$$

The Fourier coefficients live in $\mathbb{Q}(\sqrt{-1})$, and we have written $\zeta = \sqrt{-1}$ to avoid a conflict of notation. Since $M = 5$ and $\frac{N}{M} = 2$, all three conditions of Proposition 5.1 must be checked. One finds, for instance, that (f, i) and $(\bar{f}, k - i)$ satisfy (H-cyc') for $p = 7$ whenever $6 \nmid (i - 3)(1 - i)$.

Acknowledgements The authors thank Antonio Cauchi, Meng Fai Lim, and Sujatha Ramdorai for helpful discussions during the preparation of this article. We also thank the anonymous referee for their helpful and constructive comments and suggestions, which have greatly helped improve the exposition of the article.


References

1. Ahmed, S., Lim, M.F.: On the algebraic functional equation of the eigenspaces of mixed signed Selmer groups of elliptic curves with good reduction at primes above p . *Acta Math. Sin.* **37**, 1–17 (2020)
2. Aribam, C.S.: On the μ -invariant of fine Selmer groups. *J. Number Theory* **135**, 284–300 (2014)
3. Coates, J., Sujatha, R.: Fine Selmer groups of elliptic curves over p -adic Lie extensions. *Math. Ann.* **331**(4), 809–839 (2005)
4. Coates, J., Sujatha, R.: *Galois Cohomology of Elliptic Curves*, 2nd edn. Published by Narosa Publishing House, New Delhi (2010)
5. Deligne, P.: Formes modulaires et représentations ℓ -adiques. *Séminaire Bourbaki*, 21 (1968/69), Exp. No. 355, 139–172
6. Diamond, F., Im, J.: Modular forms and modular curves, In: *Seminar on Fermat's Last Theorem* pp. 39–133. Providence, RI (1995)
7. Greenberg, R.: Iwasawa theory for p -adic representations. In: *Algebraic Number Theory*, vol. 17 of *Advanced Studies in Pure Mathematics*. Academic Press, Boston, MA, (1989), pp. 97–137
8. Jha, S., Sujatha, R.: On the Hida deformations of fine Selmer groups. *J. Algebra* **338**, 180–196 (2011)
9. Kato, K.: p -adic Hodge theory and values of zeta functions of modular forms. *Astérisque*, 295 (2004), 9, 117–290. *Cohomologies p -adiques et applications arithmétiques. III*
10. Kurihara, M., Pollack, R.: Two p -adic L -functions and rational points on elliptic curves with supersingular reduction. In: *L -Functions and Galois Representations*, vol. 320 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, (2007), pp. 300–332
11. Lei, A.: Iwasawa theory for modular forms at supersingular primes. *Compos. Math.* **147**(3), 803–838 (2011)
12. Lim, M.F.: On the control theorem for fine Selmer groups and the growth of fine Tate–Shafarevich groups in \mathbb{Z}_p -extensions. *Doc. Math.* **25**, 2445–2471 (2020)
13. Loeffler, D., Weinstein, J.: On the computation of local components of a newform. *Math. Comput.* **81**(278), 1179–1200 (2012)
14. Nakamura, K.: Local ε -isomorphisms for rank two p -adic representations of $\text{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ and a functional equation of Kato's Euler system. *Camb. J. Math.* **5**(3), 281–368 (2017)
15. Nakamura, K.: Zeta morphisms for rank two universal deformations, 2020. preprint, [arXiv:2006.13647v2](https://arxiv.org/abs/2006.13647v2)

16. Perrin-Riou, B.: Représentations p -adiques et normes universelles. I. Le cas cristallin. *J. Am. Math. Soc.* **13**(3), 533–551 (2000)
17. Rubin, K.: Euler systems, vol. 147 of *Annals of Mathematics Studies*. Princeton University Press, Princeton, NJ, (2014). Hermann Weyl Lectures. The Institute for Advanced Study
18. The Sage Development Team. Sage Mathematics Software (Version 9.0), (2020). <http://www.sagemath.org>
19. Tate, J.: Duality theorems in Galois cohomology over number fields. In: *Proceeding of the International Congress of Mathematicians*. (Stockholm, 1962) (1962), pp. 288–295
20. Weston, T.: Unobstructed modular deformation problems. *Am. J. Math.* **126**(6), 1237–1252 (2004)
21. Wuthrich, C.: The fine Selmer group and height pairings. PhD thesis, University of Cambridge (2004)
22. Wuthrich, C.: Iwasawa theory of the fine Selmer group. *J. Algebraic Geom.* **16**(1), 83–108 (2007)

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Authors and Affiliations

Jeffrey Hatley¹ · Debanjana Kundu² · Antonio Lei³  · Jishnu Ray⁴

Jeffrey Hatley
hatleyj@union.edu

Debanjana Kundu
dkundu@math.ubc.ca

Jishnu Ray
jishnu.ray@tifr.res.in, jishnuray1992@gmail.com

- ¹ Department of Mathematics, Union College, Bailey Hall 202, Schenectady, NY 12308, USA
- ² Pacific Institute of Mathematical Sciences, University of British Columbia, 4176-2207 Main Mall, Vancouver, BC V6T 1Z4, Canada
- ³ Département de Mathématiques et de Statistique, Université Laval, Pavillion Alexandre-Vachon, 1045 Avenue de la Médecine, Québec, QC G1V 0A6, Canada
- ⁴ School of Mathematics, Tata Institute of Fundamental Research, Dr Homi Bhabha Road, Navy Nagar, Colaba, Mumbai, Maharashtra 400005, India